



Claire McCaskill

Missouri State Auditor

---

May 2005

# OFFICE OF STATE COURTS ADMINISTRATOR

## Justice Information System Data Integrity



**Statewide court record database has valid data, but shared accounts and passwords leaves confidential information vulnerable to exposure**

This audit reviewed how well the statewide court records system - known as the Justice Information System - is keeping information accurate, valid and secure from unauthorized access. Because court records include confidential and sealed cases, data integrity and security are vital. As of December 2004, the state had spent \$99 million on court automation and 82 of 120 courts in the state were connected to the system. The system tracks court case information and is administered by the Office of State Courts Administrator (OSCA).

---

System alerts ensure court data is accurate and valid

Auditors tested the system by trying to enter incorrect data, such as dates in the wrong format, letters in a dollar field or wrong codes in certain fields. Auditors found the edit checks functioned properly by not allowing the incorrect data to be accepted. (See page 5)

---

Shared accounts opens system to unauthorized access

Auditors found OSCA employees responsible for administering and securing the system share system accounts and passwords. Accepted security standards call for segregation between security and database administrative duties. (See page 6)

---

Local courts do not see security violation reports

Local courts using the system have not had the opportunity to review security violations occurring in their courts. Instead, an OSCA employee reviews violation reports, but only shares consistent violations. Accepted security standards state access violations and security activity should be reviewed regularly. While an OSCA employee may review security violation reports, it is important for local court officials to review security violations because they may be more likely to recognize security concerns occurring in their courts. (See page 6)

---

Local courts need ability to verify users and access rights

Local courts do not have complete and accurate information to verify users and their access rights. Periodic comparison of users and rights will maintain effective control over access and reduce the risk of fraud. (See page 7)

---

Passwords are not kept private or limited to one user

Unauthorized access to the system could occur because OSCA security administrators have access to each user's password. The administrators could use information in the password file to masquerade as another user to access court data. Accepted security standards state passwords are most effective when they are kept confidential and limited to one user. (See page 8)

**All reports are available on our website: [auditor.mo.gov](http://auditor.mo.gov)**



**CLAIRE McCASKILL**  
**Missouri State Auditor**

Honorable Matt Blunt, Governor  
and  
Michael Buenger, State Courts Administrator  
Office of State Courts Administrator  
Jefferson City, MO 65102

The Office of State Courts Administrator (OSCA) is responsible for administering the Justice Information System (JIS) used to support the automated case management activities for the state court system. Since court records include confidential and sealed cases, JIS data integrity and security are vital. Our objectives included determining whether controls to validate and edit JIS information have been effective, and whether court case data maintained in the JIS has been properly protected against unauthorized access, and accidental or intentional destruction and disclosure.

We found controls to validate and edit data in JIS have been working effectively to help ensure the accuracy of court information in JIS. However, we identified weaknesses in security practices that may affect the integrity of JIS. We found system administration user accounts have been shared, security duties have not been properly segregated from other administration duties, and local court officials have not had the opportunity to review and monitor security violations for their courts nor have they been provided a complete and accurate list of JIS users and access rights for review. In addition, knowledge of user passwords has not been limited to the user.

We have included recommendations to improve the security of JIS, which should allow OSCA to further enhance the integrity of court case management information.

We conducted our work in accordance with Government Auditing Standards issued by the Comptroller General of the United States. This report was prepared under the direction of Kirk Boyer, Director. Key contributors to this report were Jeff Thelen, Lori Melton, and Frank Verslues.

Claire McCaskill  
State Auditor

---

# Contents

---

<b>Security Risks May Compromise the Integrity of Court Case Data</b>	Background	3
	Scope and Methodology	4
	Adequate Data Validation and Edit Controls Implemented	5
	System Accounts Have Been Shared and Duties Have Not Been Properly Segregated	6
	No Security Violations Report Available for Review by Local Court Officials	6
	No Complete and Accurate List of JIS Users and Access Rights Available for Review	7
	Knowledge of Passwords Not Limited to Individual User	8
	Conclusions	9
	Recommendations	10
	Agency Comments	10
<hr/>		
<b>Appendix I</b>	Division of Responsibility	11
<hr/>		
<b>Appendix II</b>	Agency Comments	12

---

## Abbreviations

GAO	Government Accountability Office
JIS	Justice Information System
OSCA	Office of State Courts Administrator

---

# Security Risks May Compromise the Integrity of Court Case Data

---

OSCA controls to validate and edit data in JIS have been working effectively to help ensure the accuracy of court information entered in the system. However, the management practices to administer user accounts<sup>1</sup> have not always ensured JIS data is properly protected against unauthorized access and disclosure. This has occurred because system administration user accounts have been shared, security administration duties have not been properly segregated from other administration duties, and local court officials have not had the opportunity to review and monitor JIS security violations for their courts nor have they been provided a complete or accurate list of JIS users and access rights for review. In addition, knowledge of system user passwords has not been limited to individual system users.

---

## Background

OSCA has responsibility for providing administrative and technical support to Missouri courts. In 1994, OSCA began work on a statewide court automation program<sup>2</sup> to connect and automate 120 courts in the state. As of December 2004, OSCA had spent approximately \$99 million<sup>3</sup> on the program and had installed JIS, a commercial product, in 82 courts.<sup>4</sup>

OSCA relies extensively on JIS to process and store court cases, financial information, and other data. Each circuit, the three appellate courts, the Supreme Court and the centralized fine collection center has a separate JIS application and database to process and store its own case data. To help local court users or to view a court's records, OSCA staff must log on to the individual JIS application and database for that court. Both OSCA staff and local court staff have responsibilities for JIS data integrity and security. OSCA is responsible for system upkeep and maintenance, as well as staffing help desks for the courts to call with questions. The courts are responsible for case management, accounting, and scheduling. Appendix I presents a detailed breakdown of the main responsibilities OSCA and the local courts have for the security, operation and maintenance of JIS.

---

<sup>1</sup> Per accepted standards, user account administration involves (1) the process of requesting, establishing, issuing, changing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

<sup>2</sup> Section 476.055, Missouri Revised Statutes 2000 provides for a statewide court automation program.

<sup>3</sup> The money spent included \$42.5 million from a statewide court automation fee, \$56 million from the General Revenue Fund, and \$573,077 from the Crime Victims' Compensation Fund.

<sup>4</sup> The 82 jurisdictions included 76 counties (making up 31 circuits), the City of St. Louis, the three appellate courts, the Supreme Court and the centralized fine collection center for traffic tickets.

---

Data integrity exists when data agrees with its source and has not been accidentally or maliciously modified, altered, or destroyed. Data integrity also exists when data and information are changed only in a specified and authorized manner. Integrity is lost if unauthorized changes are made to the data or system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the reliance of an information technology system. The controls necessary to maintain data integrity include security to restrict access and validation and edit controls to ensure the accuracy and completeness of data entered in a system.

JIS assigns a security level to each court case type ranging from data made available to the public to court sealed case information. Court users and their access levels are authorized by a local court official, which is usually the circuit clerk or a presiding judge. Once authorized, users are assigned an access level, which determines what types of cases they can access. Users from one circuit do not have access to the data from another circuit. Users can also be limited to what they may access in their own circuit.

JIS court case data must be protected against unauthorized access and disclosure to maintain data integrity and confidentiality. Protecting against these security threats is accomplished through the deployment of logical security and access controls. Logical security and access controls restrict the access capabilities of users of the system and prevent unauthorized users from accessing the system. The purposes of limiting access to data and information are to ensure:

- Users have only the access needed to perform their duties,
- Access to sensitive data, such as juvenile court cases and cases sealed by the court, is limited to very few individuals, and
- Employees are restricted from performing incompatible functions or functions beyond their responsibility.

---

## Scope and Methodology

To understand JIS data integrity and security controls, we reviewed OSCA policy and procedures, user manuals, training manuals, and we interviewed the security administrator and other OSCA staff.

We obtained access to a JIS test environment to test and evaluate the data integrity controls which validate and edit data entered in the system. We attempted to enter data containing errors and performed incorrect

---

transactions to verify JIS would reject and not accept the data or transactions.

We based our evaluation on applicable federal, national, and international standards and best practices related to information technology security controls and data integrity from the following sources:

- National Institute of Standards and Technology
- Information Systems Audit and Control Association
- U.S. Government Accountability Office (GAO)
- U.S. Department of Justice

To obtain information from local courts regarding use of JIS, we visited the courts in Boone, Cole and Macon Counties and interviewed local court officials.

To identify terminated state employees with JIS access, we obtained a list from the statewide accounting system of all individuals paid by OSCA that had a terminated status in the system. We compared this list to a list of users with active JIS user accounts. Since an employee may be terminated from state employment but still be paid by and work for the local jurisdiction, we contacted each jurisdiction to determine whether the individuals still worked at the local court or were terminated. This test was limited to individuals paid by the state and did not include terminated individuals who had been paid solely by the local jurisdictions.

We requested comments on a draft of our report from the State Courts Administrator, and those comments are reprinted in Appendix II. We conducted our work between October 2004 and January 2005.

---

## Adequate Data Validation and Edit Controls Implemented

The JIS has programmed validation rules and edit checks for all required information needed to process a transaction. Programmed validation rules and edit checks are critical controls in assuring the initial recording of data into the system is accurate, according to GAO. While JIS cannot ensure all input data is accurate or correct, validation rules and edit checks help ensure the correct data type or allowed code values have been input. For example, dates must be a certain format, letters cannot be entered in dollar fields, and only certain code values are allowed in some fields.

We performed tests on the programmed validation rules and edit checks by entering transactions in the test JIS database. We found the rules and edit checks operated effectively by not allowing the input errors or incorrect transactions we attempted to input. These programmed validation rules and edit checks also prohibit a user from saving or processing a transaction until

---

all required fields have data. The JIS User Manual also documents the policies and procedures for data input and the required information needed for the various types of case transactions.

---

## System Accounts Have Been Shared and Duties Have Not Been Properly Segregated

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure or deletion, according to GAO. Organizations can protect this critical information by granting employees the authority to read or modify only those programs and data they need to perform their duties.

OSCA security guidelines state all users should have unique system accounts and accounts should not be shared. Accepted standards also require that each user should have a unique account to ensure adequate identification. However, OSCA employees with security administration duties and employees with database administration duties share the system accounts and passwords needed to administer user accounts. The security administrator said JIS has not allowed other user accounts to be granted the authority to administer user accounts. According to OSCA management, granting security administration authority to more users would require the JIS vendor to make modifications to the system software.

Accepted standards state security administration duties should be segregated from database administration duties to reduce the risk that erroneous or fraudulent transactions could be processed and to exclude the possibility for a single individual to subvert critical controls. However, database administrators have served as backups when security administration staff have been gone, according to OSCA management. As specified in job descriptions, the database administrators have been authorized to install, configure, and administer database software, perform programming duties, and maintain user accounts.

---

## No Security Violations Report Available for Review by Local Court Officials

Accepted standards state user access violations and security activity should be logged, reported, reviewed and appropriately evaluated on a regular basis to identify and resolve incidents involving unauthorized activity. Security violations occur when users attempt to access data they are not authorized to access or perform a task they are not authorized to perform. In addition, to prevent users from having all of the necessary authority or access to perform unauthorized activity, security personnel who administer user access should not review and evaluate security violations, according to accepted standards.

Local court appointing authorities have not had the opportunity to review and monitor JIS security violations that could occur in their courts. Instead, the OSCA security administrator stated she periodically reviews the security



---

violation log for each local court's JIS database and does not share the violation information unless a consistent violation is noted. In addition, local authorities have not had access to the security violation log because the shared system administration account must be used to access the log, according to the OSCA security administrator. The security administrator said when she notices a consistent violation on a security log, such as an unauthorized user regularly trying to access something, she will call the applicable court official to alert them of the situation. However, she could not remember the last time a security problem had been noted.

A properly functioning security monitoring program is essential to ensure unauthorized attempts to access critical data are detected and investigated, according to GAO. A program would include having local court officials routinely reviewing security violations including failed attempts to access sensitive data and resources. These actions are critical for ensuring improper access to sensitive information is detected on a timely basis.

---

## No Complete and Accurate List of JIS Users and Access Rights Available for Review

Monitoring users and their access is a continuing process. New user accounts are added while others are deleted and user access may change permanently or temporarily. Keeping system user and access information up-to-date allows timely monitoring to limit users' access to only those functions necessary to accomplish their assigned responsibilities.

Management needs a control process in place to periodically verify all user accounts and user access rights, according to accepted standards. Periodic comparison of users and access rights with recorded accountability is necessary to maintain effective control over access to data and information services to reduce the risk of errors, fraud, misuse or unauthorized alteration. These accepted standards state a review of users and access rights should examine the levels of access individuals have, whether the access is needed to perform their duties, whether all accounts are still active, and whether management authorizations are up-to-date.

OSCA has not provided local court officials with complete and accurate information needed to verify users and their access rights. The security administrator told us JIS does not have the capability to produce one report that lists all users and their access rights. To monitor user access, she told us she maintains user access information in a database outside of JIS, and has not requested OSCA information technology staff to create a JIS report with this information.

OSCA's security administrator has maintained user information in a database for use by the local court officials to verify user's access rights. However, she acknowledged this user information has not been accurate

---

because she has not had time to update the database. Our review of the security administrator's database confirmed the incomplete and inaccurate information. We found users' access rights in the administrator's database differed from rights recorded in JIS. In addition, we found JIS users that had not been included on the administrator's database, and 11 terminated employees still had access to JIS.

---

## Knowledge of Passwords Not Limited to Individual User

According to accepted standards, access controls such as passwords are key to ensuring only authorized individuals gain access to data. Passwords provide a method of validating a user's identity to establish access rights. Moreover, passwords are most effective when they are kept confidential and limited to an individual user. OSCA policy requires users to not disclose their passwords to anyone, and to change their passwords if another person receives their password.

OSCA password management controls have not been sufficient to prevent unauthorized access to JIS data since the security administrator and a backup have had access to each user's password. This situation has occurred because they enter passwords in the security management database containing information on users and their access rights. The passwords have been encrypted and stored in a file which only the security administrator and backup can access. Because these individuals have had access to read the password file, they could use this information to masquerade as another user to gain unauthorized access to court case data.

---

## JIS password capability has been limited

JIS has not had the capability to require passwords which meet accepted standards. JIS has allowed users to change their passwords; however, OSCA management disabled this capability because JIS could not require users to create passwords which met OSCA policy<sup>5</sup> or accepted standards. Instead, the security administrator assigns passwords to ensure they meet OSCA policy.

JIS is a commercial product so the vendor would have to make programming changes to increase the capability for password requirements. OSCA staff stated the vendor has no plans to change JIS password capability in the version used by OSCA and it would be cost-prohibitive to

---

<sup>5</sup> OSCA's data security guidelines require passwords be hard to guess (i.e., not a word or combination of words found in a dictionary, or associated with the user in any way such as the user's phone number or child's name), use alphabetic and alpha-numeric characters, contain a combination of lower and upper case alphabetic characters, be at least 8 characters long, and be changed on a periodic basis commensurate with the sensitivity, criticality and value of the information protected.

---

direct the vendor to make software modifications necessary to increase the capability of password controls.

---

## Conclusions

JIS has adequate data validation and edit controls to help assure the accuracy of entered data. However, missing or inadequate security controls can adversely affect the continued integrity of JIS court case data.

Security responsibilities were not segregated from database administration duties. This weakness diminished the likelihood that errors and unauthorized acts may have been detected. As such, OSCA has limited accountability over user account changes. JIS would have to be modified by the vendor to allow these security administration functions to be granted to additional system accounts.

Local court officials did not receive a report of JIS security violations to review. While the OSCA security administrator may have reviewed security violation logs, it is important for local court officials to review security violations because they may be more likely to recognize security concerns occurring in their courts. To increase the effectiveness of security monitoring and to properly segregate duties, OSCA should periodically provide a report of security violations to the local court officials. In addition, local court officials did not receive an accurate list of JIS users and access rights to review and confirm. Complete and accurate user access information is necessary for both OSCA staff and local court officials to adequately verify the access granted to users and to confirm the continued need for such access.

The effectiveness of using passwords to restrict and control access is based on limiting knowledge of the password to an individual user. Since the security administrator maintained a centralized list of all user passwords, JIS users cannot maintain individual accountability on who accessed what data, or for what purposes. The security administrator assigns passwords to all users because the JIS password program did not meet OSCA policy or generally accepted standards. To reduce the risk of compromising passwords and unauthorized data access, the security administrator should discontinue maintaining the centralized list of user passwords.

---

## Recommendations

We recommend the State Courts Administrator:

1. Evaluate the cost of and feasibility of allowing security administration tasks to be granted to additional system accounts. Until this change can be accomplished, implement compensating controls by limiting use of the system administration accounts to security administration staff. Additional backup security administrators should be designated to maintain appropriate segregation of duties between security administration duties and other incompatible job duties.
2. Develop separate reports of security violations and users with their access rights from JIS data for use by local court officials.
3. Discontinue maintaining a centralized list of passwords.

---

## Agency Comments

OSCA's comments are included in Appendix II.

---

# Division of Responsibility

---

This appendix presents the main responsibilities OSCA and the local courts have for the security, operation, and maintenance of JIS, according to an OSCA official. OSCA is responsible for supporting the administration of the local courts and the local courts are responsible for the daily operations of court case management. Both OSCA and the local courts have responsibilities to ensure adequate controls are in place and operating effectively to maintain the integrity of court case data. This division of responsibility is described below.

The following tasks are the responsibility of staff at OSCA:

- Provide centralized security and database administration
- Grant system access once approved by the local courts
- Approve system access for OSCA staff
- Provide training, training materials, and procedure manuals for recommended use of JIS
- Staff a help desk to provide assistance to the local courts
- Perform backup functions for servers and databases located at OSCA
- Provide JIS backup procedures for local courts
- System maintenance including testing and installing JIS upgrades
- Manage networking capabilities
- Maintain adequate hardware not provided by the local courts (i.e. computer servers)
- Liaison activities and contract management with court automation program vendors

The following tasks are the responsibility of the local court officials as they relate to JIS:

- Approve system access for local court staff
- Case processing and management
- Receive, deposit and disburse monies
- Fiscal management – daily accounting for cases and end-of-month accounting for the court
- Compliance with procedures for recommended use of JIS
- Segregation of duties or a review of operations when segregation is not possible
- Physical security of court case information and the computer equipment
- Backup of local data on servers located at the court's facility
- Maintain adequate work stations (i.e. personal computers)

# Agency Comments



## SUPREME COURT OF MISSOURI OFFICE OF STATE COURTS ADMINISTRATOR

2112 Industrial Drive  
P.O. Box 104480  
Jefferson City, Missouri  
65110

**MICHAEL L. BUENGER**  
ADMINISTRATOR  
**DAVID S. COPLEN**  
DIRECTOR OF  
ADMINISTRATION  
AND BUDGET  
**NANCY GRIGGS**  
DIRECTOR OF  
COURT SERVICES  
PHONE (573) 751-4377

**JIM ROGGERO**  
DIRECTOR OF  
INFORMATION TECHNOLOGY  
**LINDA EVANS**  
DIRECTOR OF JUDICIAL  
DEPARTMENT EDUCATION  
**GARY WAIT**  
DIRECTOR OF JUVENILE AND  
ADULT COURT PROGRAMS  
FAX (573) 751-5540

April 14, 2005

Mr. Jeff Thelen  
Information Systems Audit Manager  
Missouri State Auditor's Office  
224 State Capitol  
Jefferson City, Missouri 65101

Dear Mr. Thelen:

Thank you for the opportunity to review the draft audit report titled, "Justice Information System Data Integrity." We offer the following as our response to each of the recommendations.

**Recommendation Number 1:**

Evaluate the cost of and feasibility of allowing security administration tasks to be granted to additional system accounts. Until this change can be accomplished, implement compensating controls by limiting use of the security administration account to security administration staff.

Additional backup security administrators should be designated to maintain appropriate segregation of duties between security administration duties and other incompatible job duties.

**Response:**

OSCA acknowledges the recommendation. OSCA will evaluate the cost and feasibility with the vendor of the JIS system to modify the security administration account to be granted to additional system accounts. OSCA will continue to limit access to the security administration account to individuals on an "as needed" basis.

**Recommendation Number 2:**

Develop separate reports of security violations and users with their access rights from JIS data for use by local court officials.

---

Appendix II  
Agency Comments

---

Mr. Jeff Thelen  
April 14, 2005  
Page Two

**Response:**

OSCA understands and agrees. OSCA had previously recognized this as an issue and had begun working on the development of new reports to allow appropriate security reviews.

**Recommendation Number 3:**

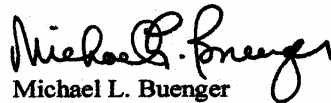
Discontinue maintaining a centralized list of passwords.

**Response:**

OSCA acknowledges the recommendation. OSCA will work with our vendor to develop password compliance in the application for the future.

We appreciate the opportunity to review the draft report. If further information or clarification is needed, please let me know.

Sincerely,

  
Michael L. Buenger

MLB/jr